Частное учреждение высшего образования
«Институт государственного администрирования»

Кафедра математики и информационных технологий

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П.Н. Рузанов
«28» февраля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Компьютерная безопасность»

Направление подготовки:
38.03.05 Бизнес-информатика
профиль:
Информационные технологии в управлении предприятием

Квалификация – бакалавр
Форма обучения: очная

Москва 2023 г.

Рабочая программа по дисциплине **«Компьютерная безопасность»**
составлена на основании требований Федерального государственного образовательного стандарта высшего образования – бакалавриат, от 29 июля 2020 г. № 838, для обучающихся по направлению подготовки **38.03.05 «Бизнес-информатика».**

Составитель:
к.т.н., доцент Верба В.А.

РАССМОТРЕНА и ПРИНЯТА
на заседании кафедры
математики и информационных
технологий
«28» февраля 2023 г., протокол № 2

В.А.Верба

(подпись)

ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Компьютерная безопасность» является изучение основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению компьютерной безопасности в сфере экономики.

Задачи:

- знаний о современных тенденциях угроз компьютерной безопасности, о нормативных правовых документах по защите информации, а так же о современных методах и средствах обеспечения компьютерной безопасности в экономических информационных системах;
- умений выявлять угрозы компьютерной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения компьютерной безопасности;
- навыков владения приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения компьютерной безопасности в социально-экономических компьютерной системах (СЭКС).

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Компьютерная безопасность» относится к части учебного плана, формируемой участниками образовательных отношений ОПОП бакалавриата по направлению 38.03.05 Бизнес-информатика.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**
	Индикатор достижения компетенции *(код, содержание индикатора*	**Результаты обучения по дисциплине**	
1	**2**	**3**	**4**
ПК-4. Способен проводить идентификацию конфигурации информационной системы	**ПК-4.1 Понимает архитектуру, устройство и функционирование информационных систем и обеспечение их компьютерной безопасности**	*Знать:* **- инструменты и методы функционирования информационных системах и обеспечение их безопасности;** *Уметь:* **- выделять инструменты и методы, подходящие к определенной информационной системе и обеспечению ее безопасности;** *Владеть* **- навыками поиска инструментов и методов защиты информации конкретной организации**	**Тестовые и ситуационные задания, кейсы**

Продолжение таблицы

1	2	3	4
	ПК-4.2 Обладает возможностями определять базовые элементы конфигурации информационных систем в соответствии с регламентом организации, в том числе компьютерной безопасности	*Знать:* **- базовые элементы конфигурации информационных систем и обеспечение их безопасности;** *Уметь:* **- выделять элементы конфигурирования, подходящие к определенной информационной системе и обеспечению ее безопасности;** *Владеть* **- навыками выбора направлений конфигурирования информационной системы организации для повышения компьютерной безопасности деятельности в соответствие с регламентом**	**Тестовые и ситуационные задания, кейсы**
	ПК-4.3 Может использовать программные средства и платформ инфраструктуры информационных технологий организаций и обеспечения их безопасности	*Знать:* **- программные средства и платформы инфраструктуры в информационных системах, способствующие обеспечению их безопасности;** *Уметь:* **- выделять программные средства и платформы инфраструктуры, подходящие к определенной информационной системе и обеспечению безопасности;** *Владеть* **- навыками поиска программных средств платформ инфраструктуры для повышения компьютерной безопасности деятельности компании**	**Тестовые и ситуационные задания, кейсы**
ПК-5. Способен разрабатывать бизнес-требования заинтересованных лиц	**ПК-5.1 Понимает теорию управления бизнес-процессами в контексте компьютерной безопасности**	*Знать:* **- инструменты и методы управления бизнес-процессами и обеспечение их безопасности;** *Уметь:* **- выделять инструменты и методы, подходящие к определенным бизнес-процессам и обеспечению их безопасности;** *Владеть* **- навыками поиска инструментов и методов защиты информации при управлении бизнес-процессами**	**Тестовые и ситуационные задания, кейсы**
	ПК-5.2 Может формулировать гипотезы о потребностях заинтересованных лиц относительно свойств системы в контексте компьютерной безопасности	*Знать:* **- основные гипотезы о потребностях заинтересованных сторон в части обеспечения компьютерной безопасности;** *Уметь:* **- выделять гипотезы, подходящие к определенной информационной системе и обеспечению ее безопасности;** *Владеть* **- навыками выбора подходящей гипотезы о потребностях для повышения компьютерной безопасности деятельности организации в соответствие с регламентом**	**Тестовые и ситуационные задания, кейсы**

Продолжение таблицы

	ПК-5.3 Может оформлять требования заинтересованных лиц по компьютерной безопасности в документе бизнес-требований	*Знать:* **- основные правила оформления требований заинтересованных лиц по компьютерной безопасности;** *Уметь:* **- выделять требования заинтересованных лиц по компьютерной безопасности и оформлять их документально;** *Владеть* **- навыками поиска формулирования и оформления требований компьютерной безопасности в бизнес-требованиях**	**Тестовые и ситуационные задания, кейсы**

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Тематический план форма обучения - очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Тема 1.Основополагающие положения	5	1-6	6	4		2	24	Рейтинг-контроль №1
2	Тема 2. Теория компьютерной безопасности	5	7-12	6	4		2	24	Рейтинг-контроль №2
3	Тема 3. Защита информации	5	13-18	6	4		2	24	Рейтинг-контроль №3
Всего за 5 семестр:				18	12		6	72	Зачет
Наличие в дисциплине КП/КР				-	-	-		-	
Итого по дисциплине				18	12		6	72	Зачет

Содержание лекционных занятий по дисциплине

Тема 1. Основополагающие положения

Международные стандарты информационного обмена. Понятие угрозы. Компьютерная безопасность в условиях функционирования в России глобальных сетей. Три вида возможных нарушений информационной системы. Защита. Современная нормативно-законодательная база обеспечения компьютерной безопасности.

Тема 2. Теория компьютерной безопасности

Назначение и задачи в сфере обеспечения компьютерной безопасности на уровне государства. Основные положения теории компьютерной безопасности. Модели безопасности и их применение. Таксономия нарушений компьютерной безопасности вычислительной системы и

причины, обуславливающие их существование. Анализ способов нарушений компьютерной безопасности.

Тема 3. Защита информации

Использование защищенных компьютерных систем. Методы криптографии. Основные технологии построения защищенных систем. Место компьютерной безопасности экономических систем в национальной безопасности страны.

Содержание практических/лабораторных занятий по дисциплине Тема

1. Основополагающие положения

Форма занятия - устный опрос, выполнение практических работ, тестирование **Практическая работа №1. Компьютерная безопасность в условиях функционирования в России глобальных сетей (2 часа)**

Стандарты в области компьютерной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и компьютерная безопасность.

Практическая работа №2. Виды противников или «нарушителей». Понятие о видахвирусов (2 часа)

Понятие нарушителя компьютерной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и ихклассификация.

Практическая работа №3. Основные нормативные руководящие документы, касающиеся компьютерной безопасности (2 часа)

Три вида возможных нарушений компьютерной безопасности. 3 составляющих ИБ -целостность, доступность, конфиденциальность. Защита компьютерной системы от угроз.

Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этойобласти. Рассекречивание документов. Уровень тайны.

Тема 2. Теория компьютерной безопасности

Форма занятия - устный опрос, выполнение практических работ, тестирование **Практическая работа №4. Назначение и задачи в сфере обеспечения компьютерной безопасности на уровне государства (2 часа)**

Схема построения компьютерной безопасности на уровне государства. Назначение иза- дачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения компьютерной безопасности государства. Военные подразделения в сфере компьютерной безопасности.

Практическая работа №5. Основные положения теории компьютерной безопасности. Модели безопасности и их применение (2 часа)

Основные положения теории компьютерной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели безопасности для домашней информационной системы. Применение методов компьютерной безопасности.

Практическая работа №6. Таксономия нарушений компьютерной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способовнарушений компьютерной безопасности (2 часа)

Понятие таксономии нарушения безопасности. Причины нарушения компьютерной безопасности. Аудит событий в рамках информационной системы. Анализ различных

способов нарушений компьютерной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.

Тема 3. Защита информации

Форма занятия - устный опрос, выполнение практических работ, тестирование

Практическая работа №7. Использование защищенных компьютерных систем (2 часа)

Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике.

Практическая работа №8. Методы криптографии. Основные технологии построениязащищенных систем (2 часа)

Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная цифровая подпись. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенностииспользования средств компьютерной защиты.

Практическая работа №9. Место компьютерной безопасности экономических системв национальной безопасности страны (2 часа)

Компьютерная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция компьютерной безопасности. Основные сведения ипоило- жения.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Текущий контроль успеваемости проводится в форме рейтинг-контроля три раза в семестр. Типовые задания для проведения текущего контроля приведены ниже.

Тестовые задания к рейтинг-контролю № 1

1. Собственником информации не может быть:

а) государство;

б) юридическое лицо;

в) группа физических лиц;

г) физическое лицо;

д) ответы а - г правильны;

е) нет правильного ответа.

2. Терминология в сфере защиты информации регулируется:

а) ГОСТ Р 6.30 - 2003

б) ГОСТ 51141 - 98

в) ГОСТ 50922 - 96

г) Гражданским кодексом.

3. Заранее намеченный результат защиты информации - это:

а) замысел защиты информации;

б) цель защиты информации;

в) уровень эффективности защиты информации.

4. Содержание и порядок действий, направленных на обеспечение защиты информации

а) мероприятие по защите информации;

б) система защиты информации

в) организация защиты информации.

5. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственникоминформации - это:

а) носитель информации

б) собственник информации

в) владелец информации

д) пользователь информации

6. В настоящее время по степени конфиденциальности можно классифицировать информацию,

а) составляющую коммерческую тайну;

б) составляющую государственную тайну;

в) составляющую служебную тайну;

г) составляющую профессиональную тайну.

7. В каких областях деятельности может быть государственная тайна

а) военной

б) образовательной

в) экономической

г) контрразведывательной

д) внешнеполитической

е) внутриполитической

ж) разведывательной

з) оперативно-розыскной

и) экологической

к) правильны все ответы.

8. Классифицированный список типовой и конкретной ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологическихновшествах - это

а) перечень ценных и конфиденциальных документов организации

б) перечень конфиденциальных сведений организации

в) перечень типовых документов, образующихся в деятельности организации.

9. Организацией конфиденциального делопроизводства непосредственно занимаются:

а) все сотрудники организации в меру своих сил и обязанностей

б) служба безопасности

в) сектор конфиденциального делопроизводства в составе службы безопасности

г) первый руководитель организации

д) постоянно действующая экспертная комиссия

е) комиссии по проверке наличия, состояния и учета документов

10. Кто имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов организации всем категориям сотрудников и другим лицам?

а) руководитель службы безопасности

б) первый руководитель организации

в) руководитель сектора конфиденциального делопроизводства в составе службы безопасности

г) правильны все варианты

11. Для работы сотруднику подразделения понадобились конфиденциальные сведения идокументы другого подразделения. Кто должен дать разрешение на ознакомление со сведениями и документами?

а) непосредственный начальник этого сотрудника

б) заместитель руководителя организации, курирующий данное направление

в) начальник подразделения, содержащего необходимые конфиденциальные сведения и документы

г) только первый руководитель организации.

12. Конфиденциальные документы уничтожаются, если

а) они являются исполненными

б) истек срок их конфиденциальности

в) истек срок их хранения

13. Отправка нешифрованного конфиденциального документа по факсу

а) не допускается

б) допускается

в) допускается, если на документе стоит гриф конфиденциальности

14. При проверках наличия конфиденциальных документов:

а) проверяют только документы, не трогая дела и иные носители конфиденциальной информации, т.к. в противном случае проверки будут очень громоздкими и долговременными

б) проверяют документы и дела, не трогая иные носители конфиденциальной информации, т.к. все, что связано с компьютерными технологиями, будет проверено специалистами по компьютерной безопасности

в) проверяют документы и дела, а также иные носители конфиденциальной информации

Дайте письменный ответ на следующие вопросы:

1. Понятие и виды конфиденциальной информации в современном российскомзаконодательстве.
2. Государственная тайна.
3. Правовой режим персональных данных. Общая характеристика Федерального закона «Оперсональных данных»
4. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».

5. Понятие и разновидности служебной и профессиональной тайн.

6. Гражданско-правовая, административная и дисциплинарная ответственность за правонарушения в информационной сфере.

Задания к рейтинг-контролю № 2

Дайте письменный ответ на следующие вопросы:

1. Служба конфиденциального делопроизводства, ее статус в структуре организации.
2. Квалификационные характеристики и требования к сотрудникам службы КД.
3. Цели и задачи, права и обязанности, нормативно-методическая база службы КД
4. Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены. Предполагаемые рубежи и уровни защиты документопотоков

Задания к рейтинг-контролю № 3

1. Программа, которая может размножаться, присоединяя свой код к другой программе,называется

a. Компилятор
b. Интернет-черви
c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате не-санкционированного доступа к информации или нарушения доступности информационной системы, называется

a. Воздействием (влиянием)
b. Потерей
c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется

a. Троянской программой
b. Червем
c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата,называется

a. Устойчивостью
b. Терпимостью по отношению к риску
c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнятькоманд

a. Две
b. Одну
c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу

Фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:

a. Статическими алгоритмами

b. Алгоритмы RMS

c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:

a. Каталоги

b. Символьные файлы

c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путемвнедрения в другие программы, называются

a. Вирусами

b. Руткитами

c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

a. Правилами безопасности

b. Требованием безопасности

c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

a. Управление риском

b. Предупреждением рисков

c. Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется

a. Мультипроцессоры типа «хозяин-подчиненный»

b. Симметричный мультипроцессор

c. Мультипроцессор с общей памятью

Дайте письменный ответ на следующие вопросы:

1. Экспертиза ценности конфиденциальных документов
2. Номенклатура конфиденциальных дел. Установление сроков конфиденциальности присоставлении номенклатуры дел.
3. Правила формирования и оформления конфиденциальных дел.

5.2. Промежуточная аттестация по итогам освоения дисциплины *(Зачет).*

Вопросы к зачету по дисциплине

1. Что такое Компьютерная безопасность?
2. Какие предпосылки и цели обеспечения компьютерной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?

4. Что включает в себя компьютерная борьба?
5. Какие пути решения проблем компьютерной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз компьютерной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз компьютерной безопасностисуществуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы компьютернойбезопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защитыинформации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификациии аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. В чем заключается контроль участников взаимодействия?
27. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
30. Какой процесс называется аутентификацией пользователя?
31. Какие схемы аутентификации вы знаете?
32. Что такое смарт-карты?
33. Какие требования предъявляются к современным криптографическим системам защитыинформации?
34. Что такое симметричная криптосистема?
35. Какие виды симметричных криптосистем существуют?
36. Что такое асимметричная криптосистема?
37. Что понимается под односторонней функцией?
38. Как классифицируются криптографические алгоритмы по стойкости?
39. В чем заключается анализ надежности криптосистем?
40. Что такое дифференциальный криптоанализ?
41. В чем сущность криптоанализа со связанными ключами?

42. В чем сущность линейного криптоанализа?
43. Какие атаки изнутри вы знаете?
44. Какая программа называется логической бомбой?
45. Какими способами можно проверить систему безопасности?
46. Что является основными характеристиками технических средств защиты информации?
47. Какие требования предъявляются к автоматизированным системам защиты третьейгруппы?
48. Какие требования предъявляются к автоматизированным системам защиты второйгруппы?
49. Какие требования предъявляются к автоматизированным системам защиты первойгруппы?
50. Какие классы защиты информации от несанкционированного доступа для средстввычислительной техники имеются? От чего зависит выбор класса защищенности?
51. Какие имеются показатели защищенности межсетевых экранов?
52. Какие атаки системы снаружи вы знаете?
53. Какая программа называется вирусом?
54. Какая атака называется атакой отказа в обслуживании?
55. Какие виды вирусов вы знаете?
56. Какие вирусы называются паразитическими?
57. Как распространяются вирусы?
58. Какие методы обнаружения вирусов вы знаете?
59. Какая программа называется монитором обращения?
60. Что представляет собой домен?
61. Как осуществляется защита при помощи ACL -списков?
62. Какой список называется перечнем возможностей?
63. Какие способы защиты перечней возможностей вы знаете?
64. Из чего состоит высоконадежная вычислительная база (TCB)?
65. Какие модели многоуровневой защиты вы знаете?
66. В чем заключается организация работ по защите от несанкционированного доступаинтегрированной информационной системы управления предприятием?
67. Какие характеристики положены в основу системы классификации информационныхсистем управления предприятием?
68. Какие задачи решает система компьютерной безопасности?
69. Какие пути защиты информации в локальной сети существуют?
70. Какие задачи решают технические средства противодействия экономическому шпионажу?
71. Какой порядок организации системы видеонаблюдения?
72. Что включает в себя защита информационных систем с помощью планирования?
73. Что такое мобильные программы?
74. Что такое концепция потоков?
75. Что представляет собой метод «песочниц»?
76. Что такое интерпретация?
77. Что такое программы с подписями?
78. Что представляет собой безопасность в системе Java ?

79. Назовите несколько примеров политик безопасности пакета JDK 1.2?

80. Какие международные документы регламентируют деятельность по обеспечению защиты информации?

81. Что понимают под политикой компьютерной безопасности?

82. Что включает в себя политика компьютерной безопасности РФ?

83. Какие нормативные документы РФ определяют концепцию защиты информации?

5.3. Самостоятельная работа обучающегося.

Самостоятельная работа студентов по изучению дисциплины включает следующие виды работ: изучение материала, изложенного на лекции; изучение материала, вынесенного на практические занятия; подготовка к практическим занятиям, выполнение индивидуального задания (реферат), подготовка презентации доклада.

Самостоятельная внеаудиторная работа по курсу включает изучение учебной и научной литературы, повторение лекционного материала, подготовку к практическим занятиям, а также к текущему контролю и промежуточной аттестации. Практические занятия предусматривают совершенствование навыков работы с первоисточниками, изучения предметной специфики курса. Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены бакалаврами в ходе самостоятельной работы. Контроль самостоятельной работы бакалавров над учебной программой курса осуществляется в ходе практических занятий методом устного опроса или ответов на вопросы тем. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме. Обучающийся должен готовиться к предстоящему практическому занятию по всем, обозначенным в программе вопросам. Не проясненные (дискуссионные) в ходе самостоятельной работы вопросы следует выписать в конспект лекций и впоследствии прояснить их на практических занятиях.

Самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Видами заданий для внеаудиторной самостоятельной работы студента выступают:

<u>для овладения знаниями:</u>

- чтение текста (учебника, первоисточника, дополнительной литературы); составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- учебно-исследовательская работа;
- использование компьютерной техники и Интернета и др. при выполнении творческих домашних заданий.

<u>для закрепления и систематизации знаний</u>:

- работа с конспектом лекций (обработка текста);
- повторная работа над учебным материалом (электронного учебника, первоисточника, дополнительной литературы);
- составление плана и тезисов ответа на вопросы промежуточного контроля;
- аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.);

- подготовка сообщений на практическом занятии и др. для формирования умений и навыков:
- подготовка сообщений по заданным темам;
- решение ситуационных (профессиональных) заданий;

Проработка вопросов, выносимых на самостоятельное изучение состоит в изучении, конспектировании и анализе литературных источников.

Методические рекомендации по самостоятельному изучению вопросов тем дисциплины:

1. Необходимо прочитать литературные источники, проанализировать качество и полноту изложения материала по изучаемым вопросам в литературных источниках.
2. Рекомендуется письменно составить свои вопросы к тексту (не менее трех).
3. Рекомендуется дать собственные комментарии прочитанному материалу, аргументацию своей интерпретации.
4. Контроль выполнения внеаудиторной самостоятельной работы осуществляется на практических занятиях, индивидуальных и групповых консультациях, защите реферата, подготовке к зачету.

Примерная тематика рефератов

1. Основные понятия и определения компьютерной безопасности. Особенности защитыинформации в социально-экономических информационных системах (СЭИС)
2. Основные методы и средства защиты информации, применяемые в корпоративныхэкономических информационных системах (КЭИС).
3. Правовые меры обеспечения компьютерной безопасности в социальноэкономических информационных системах (СЭИС).
4. Законодательные и нормативные акты Российской Федерации в области защитыинформации.
5. Использование электронных ключей для организации компьютерной безопасности в КЭИС.
6. Организационно-административные методы защиты, применяемые в социально-экономических информационных системах.
7. Формирование политики безопасности предприятия (организации).
8. Криптографические методы защиты информации. Математическое и алгоритмическоеобеспечение криптографических методов защиты информации.
9. Симметричные и асимметричные криптосистемы.
10. Электронная цифровая подпись. Использование ЭЦП в экономических системах.
11. Защита информации в компьютерных сетях. Объекты защиты информации в сети.
12. Потенциальные угрозы безопасности в Интранет. Методы защиты инфор-

мации вИнтранет.

13. Потенциальные угрозы безопасности в Интернет (и в частности, в электронойкоммерции). Методы защиты информации в сети Интернет.

14. Использование межсетевых экранов для обеспечения компьютерной безопасности вИнтернет.

15. Частные виртуальные сети (VPN). Классификация VPN.

16. Количественный подход к компьютерной безопасности. Оценка защищенности механизмов защиты.

17. Методы защиты от вредоносных программ в СЭИС.

18. Аудит компьютерной безопасности.

19. Управление информационными рисками

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ Наличие в электронной библиотеке ВлГУ (дата обращения)
Основная литература*		
Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с.	2017	http://znanium.com/catalo2/product/612572 (дата обращения: 16.06.2021)
Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2023. —	2023	
Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИН- ФРА-М, 2018. — 432 с.	2018	http://znanium.com/catalos/product/987326 (дата обращения: 16.06.2021)
Дополнительная литература		
Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шань- гин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.	2017	http://znanium.com/catalog/product/775200 (дата обращения: 16.06.2021)
Информационная безопасность конструкций ЭВМ и систем : учеб. Пособие / Е.В. Глинская, Н.В. Чичварин. — М. : ИНФРА- М, 2018. — 118 с.	2018	http://znanium.com/catalos/product/925825 (дата обращения: 16.06.2021)

6.2. Периодические издания

Журнал «Компьютерная безопасность регионов»

Журнал «Программная инженерия и информационная безопасность».

Журнал «Компьютерная безопасность и компьютерные технологии в деятельности правоохранительных органов».

Журнал «BIS Journal-Компьютерная безопасность банков ».

6.3. Интернет-ресурсы

www.inside-zi.ru/

http://elib.vlsu.ru/

http://znanium

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий практического/лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы: аудитории, оснащенные мульти-медиа оборудованием, компьютерные классы с доступом в интернет, аудитории без специального ооборудования.

Перечень используемого лицензионного программного обеспечения: пакет MS-Office, Microsoft Windows, 7-Zip, AcrobatReader; СПС «Консультант Плюс» (инсталированный ресурс ВлГУ).

Примечание:

Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов.

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей. В соответствии с нормативно-правовыми актами для инвалидов и лиц с ограниченными возможностями здоровья при необходимости тестирование может быть проведено только в письменной или устной форме, а также могут быть использованы другие материалы контроля качества знаний, предусмотренные рабочей программой дисциплины.

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20_____ / 20 ____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

Рабочая программа одобрена на 20	/ 20	учебный года
Протокол заседания кафедры №	от	года

Заведующий кафедрой

Рабочая программа одобрена на 20	/ 20	учебный года
Протокол заседания кафедры №	от	года

Заведующий кафедрой

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины **Компьютерная безопасность**

образовательной программы направления подготовки 38.03.05 Бизнес-информатика, профиль подготовки «Информационные технологии в управлении предприятием»

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			